Serial No. 09/884,672
Art Unit No. 2134

AMENDMENTS TO THE SPECIFICATION

Amend the paragraph found from page 30, line 19 through page 31, line 14 as follows:

Fig. 12 is a flowchart of communication processing on the side of destination B. First, it receives a public key Kx (step 60). Note that this received public key is referred to as Kx rather than Kp ~~Ke~~ here, because it might be tampered with by a malicious third party intervening on the transmission line between source A and destination B. Next, verification data Xx is generated from Kx based on the verification data generation algorithm specified by ID1 that was sent from source A with a public key Kp (step 62), then the verification data Xx is output to the verification image display section 27 (step 64). In step 66, own verification data Xx is compared with verification data Xp of source A, as a result, if the comparison matches, the process proceeds to step 68, while mismatches, the process is terminated for error (i.e., data integrity is not secured). If data integrity is secured, a random number R is generated (step 68), then the random number R and ID2, which is the ID of the symmetric key generation algorithm selected among a plurality of symmetric key generation algorithms this time, are encrypted using a public key of source A and transmitted to source A (step 70), then the symmetric key Kc is generated based on the symmetric key generation algorithm of ID2 (step 72), thereafter, cipher communication starts with source A using the symmetric key (step 74).